UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/621,056	07/21/2000	David W. Carman	NTWK005/05US	4462

28875 7590 02/27/2004

SILICON VALLEY INTELLECTUAL PROPERTY GROUP
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	10

DATE MAILED: 02/27/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/621,056	CARMAN ET AL.	
	Examiner	Art Unit	
	Thomas M Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 July 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5* is/are rejected.

7)☒ Claim(s) *6-12* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-12 are pending.

Claim Objections

2. Claims 6-12 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Double Patenting

3. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claim 1 rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 09/621059 and claim 1 of Application No. 09/621057. Although the conflicting claims are not identical, they are not patentably distinct from each other because the two claims of 09/621056 and 09/621059 read on each other.

Claim 1 of 09/621056 reads:

A method for generating an authentication tag for a message that can be used for error correction processing comprising:

- Processing a portion of the message using a reversible first function to produce an intermediate result.
- Processing the intermediate result with a second function to produce the authentication tag.

Claim 1 of 09/621059 reads:

A method for generating an authentication tag for a message, comprising:

- Processing a portion of a message using a first function to produce an interim output.
- Processing the interim output using a second function to produce the authentication tag.

While Claim 1 of 09/621059 recites processing a portion of a message using a first function and Claim 1 of 09/621056 recites a "reversible first function", it is understood that a reversible first function is still a function and is not patentably distinct over from 09/621059. Additionally the method for generating an authentication tag that can be used for error correction (09/621056) is still a method for generating an authentication tag (09/621059).

It would have been obvious to one of ordinary skill in the art at the time of invention to process a message using a reversible first function (such as an XOR) to generate an authentication tag given that many functions used in error correction make use of reversible functions, since it would allow some of the lost information to be restored (parity checks).

Claim 1 of 09/621057 reads:

An authentication system, comprising:

- A plurality of inner functions that are operative on a respective plurality of collections of message parts to produce a plurality of intermediate outputs
- An outer function that is operative on said plurality of intermediate outputs to generate an authentication tag.

Claim 1 of 09/621057 is obvious over claim 1 of 09/621056, the only difference being that claim 1 of 09/621057 claims a plurality of these inner function, and consequently a plurality of inputs and outputs.

It would have been obvious to one of ordinary skill in the art at the time of invention to apply the authentication system computation of claim 1 (09/621057) only once, to produce an

authentication tag from a "portion of a message using a reversible first function to produce an intermediate result", for the advantage of producing a singular authentication tag when only one is needed rather than a plurality of them.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-5 are rejected under 35 U.S.C. 102(a) as being anticipated by Balenson et al.

In reference to claim 1:

Balenson et al. (Page 19, Figure 4) discloses a method for generating an authentication tag for a message that can be used for error correction comprising:

- Processing a portion of the message using a reversible first function to produce an intermediate result, where the intermediate result comes out of the computation of the inner mac.
- Processing the intermediate result with a second function to produce the authentication tag, where the second function is the outer MAC, and the outer MAC creates an authentication tag.

In reference to claim 2:

Balenson et al. (Fig. 9, page 33) discloses a method further comprising encrypting the intermediate result, where the intermediate result is the enciphering, or encryption by DES. DES or Digital Encryption Standard encrypts the message at each point in the intermediate computation of the MAC.

In reference to claim 3:

Balenson et al. (page 33-34, Figs 9 & 10) discloses a method further comprising sending the intermediate result to the receiver of the message, where the receivers of the messages are the intermediate modules in the computation of DES-MAC or RC6.
DES-MACs or other iterative inner functions such as RC6, perform such that one intermediate result in the computation of the inner function is sent to the next module, where the next iteration is performed. Because the message information passes through the inner functions, and the outer functions, these inner DES modules, although used to computer a final Inner or Outer MAC are also receivers of the message.

Additionally, it was well known in the art at the time of invention that a single functional computation may be processed over several computers in situations where a single computer has insufficient resources or security clearance to complete a computation. Subsequent computers, used in the computation of a single function are also receivers to which the encrypted intermediate results may be performed.

In reference to claim 4:

Balenson et al. (page 8, Figure 1) discloses a method further comprising sending the authentication tag to the receiver, where the tag created by the sender is sent to the receiver.

In reference to claim 5:

Balenson et al. (Figure 1, page 8) discloses a method for detecting errors in a message comprising:

- Receiving at least one message data word and an authentication tag, said authentication tag produced from said at least one message data word according to a nested message authentication code having a reversible inner function, where the embodiment of the nested message authentication code appears on (Figure 4, page 19.)
- Processing said received at least one message data word according to said nested message authentication code to produce an authentication tag, where the receiver of the message (Figure 4, page 19.)
- Determining whether said production authentication tag is the same as said received authentication tag, (Figure 1, page 8) where this is determined on the receiver side.

6. Claims 1, 5 are rejected under 35 U.S.C. 102(b) as being anticipated by Bellare et al.

In reference to claim 1:

Bellare et al. (The Nested Construction, NMAC, page 9) discloses a method for generating an authentication tag for a message that can be used for error correction comprising:

- Processing a portion of the message using a reversible first function to produce an intermediate result, where the intermediate result is $F_{k2}(x)$.
- Processing the intermediate result with a second function to produce the authentication tag, where an NMAC is still a MAC, and the final output is an authentication tag.

In reference to claim 5:

Bellare et al. (Authenticity and MACs, page 2, and The Nested Construction NMAC, page 9) discloses a method for detecting errors in a message comprising:

- Receiving at least one message data word and an authentication tag, said authentication tag produced from said at least one message data word according to a nested message authentication code having a reversible inner function, where party A transmits a message to party B with the authentication tag, with reversible inner function from the NMAC.
- Processing said received at least one message data word according to said nested message authentication code to produce an authentication tag, where the authentication tag is recomputed at party B.
- Determining whether said production authentication tag is the same as said received authentication tag, where the second party B "checks that the value he obtains is equal to the tag attached to the received message"

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

February 12th 2003

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100